

Computer Mapping and Data Protection

A joint publication by NIJ's
Crime Mapping Research Center and
the Institute for Law and Justice

July, 2000

Chapter V Outline

V. Sharing Data with Researchers

- A. Police departments have provided researchers with crime data in the past.
 - 1. Most of the data was in the public record and therefore posed no privacy risks.
 - 2. Aggregate data were sometimes provided, rather than individual records.
- B. The difference now is that the geocoded data, while still technically in the public record, provides much more precise information than past data given to researchers. Examples are addresses of victims, known gang members, arrestees, etc.
- C. Here are some general guidelines:
 - 1. Determine the type, format and nature of the data required to do the research.
 - 2. Decide how the results of the research will be presented.
 - 3. Perform background checks on research personnel having access to data.
 - 4. Decide where data will be stored.
 - 5. Require researchers to destroy raw data after the research is completed.

- D. Here are some questions and issues that a researcher can expect to be faced with when requesting geocoded data:
1. Does the research add value to the policing profession?
 2. What do I know about the researcher and what can I find out?
 3. Are the results likely to embarrass the department?
 4. Will the researcher guarantee that the data will be used only for the agreed upon research purpose?
 5. Make arrangements for regular meetings between the researchers and police personnel to discuss the project, including the interpretation of data analysis and maps.
- E. You may want to consider a Memorandum of Understanding with the research organization on the use of the research project, including the use of the data.